

CLAIMS

- 1 1. A decoder for processing a transport packet stream comprising packetised data
2 encapsulated within the packet payloads, said decoder comprising:
3 means for receiving an identifier of a particular security module system from a
4 portable security module;
5 means for configuring the decoder in response to the received identifier;
6 means for receiving filter data for filtering packetised data associated with said
7 particular security module system from the portable security module; and
8 means for filtering said packetised data in response to said received filter data.
- 1 2. A decoder according to Claim 1, wherein the filtering means is configurable by said
2 configuring means to extract from the packetised data data associated with said particular
3 security module system for subsequent filtering in response to said received filter data.
- 1 3. A decoder according to Claim 1, wherein said identifier comprises an identifier of a
2 particular conditional access system.
- 1 4. A decoder according to Claim 3, wherein the filtering means is adapted to
2 extract from the packetised data transport packets containing a program map table and a
3 conditional access table.
- 1 5. A decoder according to Claim 4, wherein the configuring means is adapted to
2 receive the program map table and conditional access table from the filtering means and
3 configure the filtering means in response to the received identifier and data contained in the
4 program map table and the conditional access table.
- 1 6. A decoder according to Claim 1, wherein said identifier comprises an identifier of a
2 particular debiting system used by the security module.

1 7. A decoder according to Claim 1, wherein said identifier comprises an identifier of a
2 particular crediting system used by the security module.

1 8. A decoder according to Claim 1, wherein the filtering means is configurable in
2 response to filter data comprising at least a table identifier or a section identifier for the
3 packetised data.

1 9. A decoder according to Claim 1, wherein the filtering means comprises first
2 filtering means for extracting from the packetised data data associated with said particular
3 security module system and second filtering means for filtering the extracted data in
4 response to said filter data.

1 10. A decoder for processing a transport packet stream comprising packetised data
2 encapsulated within the packet payloads, said decoder comprising:
3 first filtering means for extracting from the packetised data data associated with a
4 particular security module system; and
5 second filtering means for filtering the extracted data in response to filter data
6 received from a portable security module.

1 11. A decoder according to Claim 10, wherein the first filtering means is configurable
2 in response to an identifier of said particular security module system received from said
3 security module.

1 12. A decoder according to Claim 9, wherein said second filtering means comprises a
2 plurality of filters, at least one of said filters being configurable in response to said filter
3 data.

1 13. A decoder according to Claim 9, wherein said second filtering means is
2 configurable in response to a data pattern included in said filter data.

- 1 14. A decoder according to Claim 13, wherein said second filtering means is
2 configurable to filter from the extracted data data having a pattern matching said data
3 pattern included in the filter data.
- 1 15. A decoder according to Claim 13, wherein said second filtering means is
2 configurable to not filter from the extracted data data having a pattern matching said data
3 pattern included in the filter data.
- 1 16. A decoder according to Claim 13, wherein said second filtering means is
2 configurable to ignore at least part of said data pattern in response to a data masking pattern
3 included in said filter data.
- 1 17. A decoder according to Claim 1, comprising means for forwarding to the security
2 module conditional access data included in the packetised data.
- 1 18. A decoder according to Claim 17, wherein the conditional access data forwarded to
2 the security module comprises entitlement control messages (ECMs) and/or entitlement
3 management messages (EMMs).
- 1 19. A decoder according to Claim 1, wherein the filter data provided by the security
2 module comprises data used by the filtering means to extract group and/or individual
3 entitlement management messages addressed to the security module.
- 1 20. A decoder according to Claim 17, wherein the decoder is adapted to receive a
2 control word generated by the security module in response to the conditional access data
3 forwarded thereto, the control word being used by the decoder to descramble a scrambled
4 transmission.
- 1 21. A decoder according to any Claim 1 adapted to encrypt and/or decrypt
2 communications to and from the portable security module.

1 22. A portable security module for use with a decoder as claimed in Claim 1, said
2 security module comprising memory means for storing an identifier of a particular system
3 of the security module and means for communicating the identifier
4 to the decoder to configure the decoder.

1 23. A portable security module according to Claim 22, comprising means for storing
2 filter data and means for communicating the filter data to filtering means in the decoder.

1 24. A portable security module according to Claim 22 comprising a smartcard.

1 25. A method of processing a transport packet stream comprising packetised data
2 encapsulated within the packet payloads, said method comprising the steps at a decoder of:
3 receiving an identifier of a particular security module system from a portable
4 security module;
5 configuring the decoder in response to the received identifier;
6 receiving filter data for filtering packetised data associated with said particular
7 security module system from the portable security module; and
8 filtering said packetised data in response to said received filter data.

1 26. A method according to Claim 25, wherein the packetised data is filtered to extract
2 data associated with said particular security module system.

1 27. A method according to Claim 25, wherein said identifier comprises an identifier of
2 a particular conditional access system.

1 28. A method according to Claim 27, wherein transport packets containing a program
2 map table and a conditional access table are extracted from said packetised data.

1 29. A method according to Claim 28, wherein the packetised data is filtered in response
2 to the received identifier and data contained in the program map table and the conditional
3 access table.

1 30. A method according to Claim 25, wherein said identifier comprises an identifier of
2 a particular debiting system used by the security module.

1 31. A method according to Claim 25, wherein said identifier comprises an identifier of
2 a particular crediting system used by the security module

1 32. A method according to Claim 25, wherein the filter data comprises at least a table
2 identifier or a section identifier for the packetised data.

1 33. A method according to Claim 25, wherein the packetised data is filtered according
2 to a data pattern included in the filter data.

1 34. A method according to Claim 33, wherein data having a pattern matching said data
2 pattern is filtered from the packetised data.

1 35. A method of processing a transport packet stream comprising packetised data
2 encapsulated within the packet payloads, said method comprising the steps at a decoder of:
3 extracting from the packetised data data associated with a particular security
4 module system; and
5 filtering the extracted data in response to filter data received from a portable
6 security module.

1 36. A method according to Claim 35, wherein an identifier of said particular security
2 module system is received from said security module.

1 37. A method according to Claim 25, wherein conditional access data included in the
2 extracted data is forwarded to the security module.

1 38. A method according to Claim 37, wherein the conditional access data forwarded to
2 the security module comprises entitlement control messages (ECMs) and/or entitlement
3 management messages (EMMs).

39. A method according to Claim 25, wherein the filter data provided by the security module comprises data used by the decoder to extract group and/or individual entitlement management messages addressed to the security module.

1 40. A method according to Claim 37, wherein the a control word is generated by the
2 security module in response to the conditional access data forwarded thereto, the control
3 word being used by the decoder to descramble a scrambled transmission.

THE BIBLE